REMARKS

By the present Amendment, Claims 1-5, 7-9, 15, 16, 23, 29-33 and 35 are amended and claims 6, 22 and 36-42 are cancelled without prejudice or disclaimer. New claims 43-46 are added. The pending claims are believed to be allowable over the prior art of record and are amended herein solely for purposes of improved clarity. No new matter has been added. Reexamination and reconsideration is respectfully requested.

Embodiments of the present invention are shown, for example, with reference to Figures 1-3 of the present application. In the illustrated embodiments, a "packet processor" device (104 in Fig. 1, 204 in Fig. 2 or 304 in Fig. 3) is connected, through a processor bus 102, to a computer processor 100 and memory 101 to provide encryption and/or authentication services to the computer processor. More specifically, the computer processor 100, with memory 101, operates on data (instructions or content) communicated over the processor bus 102 in data packets. In various contexts (such as secure communication environments), it is desirable to perform encryption and/or authentication functions on data packets, before or after the computer processor 100 operates on such data packets.

The packet processor (104, 204 or 204) shown in the illustrated embodiments comprises a hardware module having a plurality of individual hardware processing units or processors (an encryption processor 108 and first and second authentication processors 110 and 112). The illustrated packet processor also includes a control unit 106. In the embodiment shown in Fig. 2, the packet processor 204 includes a local bus 202 connected between the control unit 106 and the encryption and authentication processors 108, 110 and 112. The packet processor 204 in Fig. 2 also includes a further bus, connecting the encryption and authentication processors together in a daisy-chain fashion. The hardware packet processor module 204 in Fig. 2, thus, allows the computer processor 100 to offload cryptographic and authentication functions and, thus, free the computer processor 100 to perform other tasks. In other words, data packets that would otherwise by processed for cryptographic and authentication functions by the computer processor 100 are, instead, communicated to the packet processor 204 over the processor bus 102. Under the control of the control unit 106, the plural processors 108, 110 and 112 are able to process data packets in a pipeline fashion for improved efficiency.

The use of multiple processors 108, 110 and 112, as part of a hardware module separate from the computer processor 100, allows the packet processor 204 to process multiple packets at the same time. In particular, data from the first data packet may be processed with the encryption processor 108. Thereafter, data from a second data packet may be provided to the encryption processor 108, while the encrypted data from the first packet is processed by a first authentication unit 110. Thus, with the use of multiple processors 108, 110 and 112 each connected and controlled to operate on the output of another, multiple data packets may be processed through the packet processor in a pipeline fashion.

None of the prior art of record teaches or suggests a packet processor as described and claimed. As described below, the prior art of record describes a packet processor having encryption and authentication processors or processor units connected and controlled to process packets in a pipeline fashion, as claimed.

Claims 5-8, 15, 22, 29 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wu et al. (U.S. Patent No. 5,774,551) in view of Candelore, et al. (U.S. Patent No. 6,061,449) or Anderson (U.S. Patent No. 5,911,077). With regard to cancelled Claims 6 and 22, this rejection is moot. With regard to the other rejected claims, this rejection is respectfully traversed.

Each of the rejected claims recites a method or article that includes features that are neither disclosed nor suggested by the prior art of record. For example, Claim 5 recites a method of processing data packets comprising, inter alia, receiving first and second data packets; providing a plurality of processors including at least one encryption processor and at least one authentication processor, processing the data from the first data packet with the at least one encryption processor; providing data from a second data packet to the at least one encryption processor and processing the data from the second data packet in the at least one encryption processor, while the at least one authentication processor further processes data for the first data packet. These features are not disclosed or suggested, individually or in combination, and Wu, Candelore or Anderson.

Wu is directed toward methods and systems from managing user access to network computers. In particular, Wu is concerned with authenticating a user (not encryption and authentication of data packets). Wu provides application programming interfaces (APIs) that reside between the user interface and account management services on a computer. Wu does not disclose or suggest a method which includes providing a plurality of processors, including at least one encryption processor and at least one authentication processor for processing data packets as claimed. Instead, Wu describes a system that has multiple authentication services 109, but does not include a packet data encryption service.

In the first Office Action, the Examiner pointed to column 3, lines 58-62 of the Wu patent as describing an encryption unit. However, the cited section of the Wu patent does not describe an encryption processor function as claimed (including the claimed steps of "processing said data from the first data packet with said at least one encryption processor to provide output data for the first data packet ..." and "communicating said output data for the first data packet from said at least one encryption processor to said at least one authentication processor.") Instead, Wu et al refer to a unified login scheme, in which a user's primary authentication token is used for "a primary authentication service, such as password, private key, or other unique data, to encrypt the user's other authentication tokens for other secondary authentication services." (Wu, column 3, lines 59-62) Thus, Wu's reference to encryption is a description of how a user's authentication token (not a data packet to be processed) may be encrypted. Wu does not disclose or suggest encrypting data from a first data packet and certainly does not a disclose or suggest communicating an output of an encryption processor to at least one authentication processor.

In addition, Wu does not disclose or suggest "processing the data from the second data packet in the at least one encryption processor while said at least one authentication processor further processes the output data for the first data packet," as claimed. The Examiner has acknowledged that Wu does not disclose that feature. However, the Examiner has cited the Candelore and the Anderson patents with respect to that feature. The characterization of Candelore or Anderson as describing the claimed pipeline processing method is respectfully traversed. Neither Candelor nor Anderson address the deficiencies of the Wu patent noted above.

Candelore describes a system for securely communicating encrypted blocks of program information between a storage device and a processing circuit. Although Candelore discusses simultaneous decryption and authentication of data, these operations are on the same block of data processed in parallel by two units. The system described in Candelore is a parallel processing system. In contrast, claim 5 recites that one processor operates on one data packet while another processor operates on another data packet (see the references to first and second data packets in claim 5). Thus, applicant claims a pipeline encryption and authentication process (where multiple data packets are processed) as opposed to the parallel process disclosed in Candelore (where one data packet is processed simultaneously in multiple processing units). Accordingly, even if the Candelore and Wu teachings were somehow combined (as suggested by the Examiner), the combination still would not meet the claimed invention.

Anderson describes a software system that uses interrupt processing "to permit simultaneous activation of multiple disk drives in a computer system." (Anderson, Abstract.) Anderson's software system allows two application programs running on a computer to access data files located on two separate disk drives, so that both drives are simultaneously active. (Anderson, column 4, lines 61-63.) Anderson's system employs a device driver 114 to analyze pending data request packets to determine whether the data request packets include data transfer requests to a first disc drive 110 or a second disk drive 112. In this manner, while processing the first data processing packet 160 which involves the first disk drive 110, the device driver 114 analyzes other pending data request packets to determine whether any pending data requests are associated with the second disk drive 112. If a pending data request packet is associated with the second disk drive 112, then the device driver 114 will purportedly simultaneously process that pending data request with the first data request packet. (Anderson, column 6, line 65 to column 7, line 37).

Thus, Anderson's system is designed to allow a computer to process data requests (e.g., to access data) for multiple disk drives, where data requests for data on the same disk drive are purportedly processed "simultaneously." There is no disclosure or suggestion in Anderson of processing data from a second packet in an encryption processor while simultaneously processing data for a first packet with an authentication processor. At most, Anderson appears to describe purportedly simultaneous processing of multiple data requests that involve accessing

information on multiple respective disk drives. One skilled in the art would not have considered such a teaching as rendering it obvious to somehow modify Wu to simultaneously encrypt and authenticate first and second packets. Anderson's teaching of parallel operations on the same data packet would not have led one skilled in the art to somehow modify Wu to employ multiple processors and process data from a second data packet in an encryption processor while processing data from a first data packet in an authentication processor.

Furthermore, the processor employed in a typical computer system would actually process Anderson's data requests in series (one after the other). Thus, while Anderson refers to "simultaneous" processing of requests involving the same disk drive, the actual manner in which Anderson likely operates is to process all requests for the same disk drive first (in series, not simultaneous with each other), before processing requests that involve data on another disk drive. Again, Anderson provides no suggestion or motivation to modify Wu to simultaneously encrypt and authenticate first and second packets.

Therefore, the claimed pipeline processing method (wherein data from a second data packet is processed in at least one encryption processor while at least one authentication processor processes data for a first data packet) is neither described nor suggested by Wu, Candelore or Anderson, alone or in combination. Furthermore, one skilled in the art would not have considered it obvious to modify a software system designed for user authentication (as described by Wu) to include features from a system for program code protection (as described by Candelore) or features from a software system for permitting simultaneous activation of multiple disk drives (as described by Anderson). None of the cited prior art references teach or suggest a motivation for making such a combination. Accordingly, the rejection of Claim 5 and dependent Claims 6-8 is respectfully traversed.

For similar reasons, the rejection of Claims 15, 29 and 35 is respectfully traversed. For example, Claim 15 recites, among other features, "encrypting a second data packet with the encryption processing module while authenticating the first data packet with the first authentication processing module ..." Similarly, Claim 29 recites, among other features, "encrypting a second data packet with the encryption processor while authenticating the first data packet with the first authentication processor." Also, Claim 35 recites, among other features, "providing data from the second data packet to said at least one encryption processor for processing by the at least one encryption

processor, while said at least one authentication processor further processes the output data for the first data packet."

Claims 32-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wu in view of Candelore or Anderson, and further in view of Kocher et al. (U.S. Patent No. 6,304,658). This rejection is respectfully traversed.

Claims 32-34 are dependent, directly or indirectly, on Claim 5. Accordingly, the comments regarding distinctions between Claim 5 and the Wu, Candelore and Anderson references apply to Claims 32-34 and are incorporated herein by reference. At least due to the distinctions between claim 5 and those references, it is respectfully submitted that dependent Claims 32-34 are patentably distinguished over those references. Further, the Kocher reference does not address the above-noted differences between parent claim 5 and the Wu, Candelore and Anderson references. Accordingly, dependent Claims 32-34 are patentably distinguished over Wu, Candelore, Anderson and Kocher, alone or in combination.

Kocher describes a system for securing cryptic graphic devices against attacks involving external monitoring and analysis. In Kocher, the protected cryptic graphic operation is always only one operation. There is no disclosure or suggestion in Kocher of multiple simulatenous processing operations, such as pipelining as claimed by applicant. Furthermore, it is recognized that Kocher was not cited by the Examiner for addressing such distinctions over the other cited references. Accordingly, the rejection of Claims 32-34 is respectfully traversed.

Claims 1-4, 9-14, 16-21, 23-28, 30-31 and 36-42 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wu. With regard to cancelled claims 36-42, this rejection is moot. With regard to the other rejected claims, this rejection is respectfully traversed.

Each of the rejected claims recites a method or article that includes features that are neither disclosed nor suggested by the prior art of record. For example, Claim 1 is directed to a packet processor that includes, among other features, "at least one encryption processor" and "first" and "second" authentication processors. Thus, the packet processor of claim 1 includes multiple processors (not just one processor performing multiple operations).

On the other hand, Wu describes a system that employs a computer 101 having a single Central Processing Unit 115, but not multiple processors and certainly not at least one encryption processor, a first authentication processor and a second authentication processor. In a previous Office Action (dated October 21, 2002), the Examiner stated that applicant's claims (at that time) referred to multiple processing "units" and not multiple processors. As amended herein, claim 1 now refers to "processors" (rather than processing units) and, thus, is distinguished from Wu's use of multiple authentication services 109 (software) in a computer having a single processor for implementing those services.

Claim 1 also includes a control unit that is "configured to control the at least one encryption processor and the first and second authentication processors such that a first set of data and a second set of data sent from the at least one encryption processor to the first authentication processor and the second authentication processor, respectively, are processed by the first authentication processor and the second authentication processor while the at least one encryption processor processes a third set of data." (underline added for emphasis)

Similar to the discussion above regarding claim 5, Wu does not disclose or suggest a plurality of processors, including at least one encryption processor and first and second authentication processor for processing data as claimed. Moreover, Wu does not disclose or suggest processing first and second sets of data with first and second authentication processors while processing a third set of data with at least one encryption processor.

In addition, Claim 1 further recites that the packet processor includes "a local data bus, independent of the data input to the control unit, coupling the control unit to each of the encryption and authentication processors; and a second data bus from the encryption processor to each authentication processor, including a data bus from the first authentication processor to the second authentication processor." Wu neither discloses nor suggests such data buses coupling a control unit and multiple processors, including a data bus coupling one or more encryption processors to authentication processors.

Instead, Wu describes a computer 101 that has a CPU 115 connected to an external computer or terminal through a network 139. The CPU 115 is also connected to an addressable memory 103 and to input, output, network interface or storage devices through other

connections. The addressable memory 103 contains software, including authentication service programs 109, that can be run on the CPU. Wu's CPU is not connected by a local data bus to encryption and authentication processors. Moreover, Wu does not include a second data bus from an encryption processor to first and second authentication processors. One skilled in the art would not have found it obvious to provide multiple processors and a bus connection as claimed, from Wu's storage of multiple authentication service programs in a memory coupled to a CPU.

Therefore, Claim 1 recites several features that are neither disclosed nor suggested by Wu. Claims 2-4, which are dependant on Claim 1, are patentably distinguished over Wu at least for reasons as discussed above with respect to claim 1.

Similarly, it is respectfully submitted that Claim 9 recites features that are neither disclosed nor suggested by Wu. For example, Claim 9 includes "performing encryption on a first data packet within an encryption processor" and "after completion of encryption of the first data packet, performing authentication of the first data packet within at least one authentication processor connected to the encryption processor by a data bus, and performing encryption of a second data packet within the encryption processor prior to completion of authentication of the first data packet."

As discussed above, Wu neither discloses nor suggests multiple processors including an encryption processor and at least one authentication processor connected to the encryption processor by a data bus. As noted above, Wu's description of a CPU 115 connected to a memory 100 that stores multiple authentication programs would not lead one skilled in the art to modify Wu's system to include encryption and authentication processors.

Also, while Wu describes connections of the computer 101 with a remote computer 135, the computer 101 and remote computer 135 do not perform the encryption and authentication functions of the encryption and authentication processors as claimed (i.e., wherein a first data packet is encrypted with the encryption processor and, after completion of encryption, authentication is performed on the first data packet with at least one authentication processor).

Also, as acknowledged by the Examiner, Wu does not disclose performing encryption on a first data packet and after completion of the encryption of the first data packet, performing

authentication of the first data packet and performing encryption of a second data packet prior to completion of authentication of the first data packet. While the Examiner has taken "Official notice" that encrypting a second packet before authentication is well known in the art. However, the Examiner has cited no prior art in support of that contention. Applicant respectfully traverses the rejection in that none of the prior art of record describes or suggests a method as recited in Claim 9, wherein encryption is performed on a first data packet by an encryption processor and, thereafter, authentication is performed on the first data packet with at least one authentication processor.

Furthermore, while the Examiner appears to state that parallel encryption schemes were known, where first and second packets are encrypted at the same time and where the second packet does not wait for the first packet to be authenticated. However, no prior art in support of that contention was cited. Applicant respectfully submits that such processing methods were not known prior to the present invention. Without the present disclosure as a guide, it would not have been obvious to add processors to Wu's computer 101 to perform encryption on a second data packet, before completion of authentication of the first data packet. Accordingly, the rejection of Claim 9 is respectfully traversed. Because claims 10-14 are dependent on Claim 9, directly or indirectly, the rejection of those claims is respectfully traversed at least for reasons as discussed above with respect to claim 9.

For similar reasons as discussed above with regard to Claims 1 and 9, the rejection of claims 16 and 23 is also respectfully traversed. Claim 16 recites, among other features, "one or more computer programs, performed by the computer, for performing encryption on a first data packet within an encryption processor, and, after completion of the encryption of the first data packet, performing authentication of the first data packet in at least one authentication processor connected to the encryption processor by a data bus, and performing encryption of a second data packet within the encryption processor prior to completion of authentication of the first data packet." Claim 23 recites an article of manufacture that comprises a computer program carrier with one or more computer executable instructions for performing a method similar to that of claim 9. Also, because claims 17-21 are dependent (directly or indirectly) on claim 16 and because claims 24-28 are dependent (directly or indirectly) on claim 23, the rejection of those

dependent claims is respectfully traversed at least for reasons discussed above with regard to claims 16 and 23.

Claim 30 also recites features that are neither disclosed nor suggested by Wu. For example, the method of claim 30 includes "providing a plurality of processors in data communication with the control unit over a second data bus, independent of the first data bus, said processors including at least one encryption processor and at least one authentication processor." As discussed above, Wu neither describes nor suggests plural processors that include at least one encryption processor and at least one authentication processor. Furthermore, Wu neither describes nor suggests processing data from a first data packet with said multiple processors in parallel. Instead, Wu employs a computer 101 having a single CPU 115 that implements all of the authentication processing performed by the system, using programs stored in memory 103 (where Wu refers to such programs as authentication services 109). Accordingly, the rejection of claim 30 is respectfully traversed. Also, because Claim 31 is dependent on Claim 30, the rejection of Claim 31 is respectfully traversed at least for reasons discussed above with respect to Claim 30.

Similar distinctions over the prior art are present in each of claims 36-42. Accordingly, the rejection of those claims is respectfully traversed for reasons as discussed above with respect to claims 1, 9 and 16.

Claims 36-42 are cancelled herein without prejudice, for purposes of simplifying the issues in prosecution. New claims 43-46 are added to further clarify aspects of the invention. New claims 43-46 are believed to be allowable over the prior art of record at least for reasons similar to those discussed above with respect to claims 1, 5 and 9.

In view of the forgoing, it is respectfully submitted that the application is in condition for allowance. Re-examination and reconsideration of the application, as amended, are requested.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 06-1447. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even

entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 06-1447. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 06-1447.

Respectfully submitted,

Date: December 8, 2003

By _____

FOLEY & LARDNER
Customer Number: 23392
PATENT TRADEMARK OFFICE
Telephone: (310) 975-7963
Facsimile: (310) 557-8475

Ted R. Rittmaster
Attorney for Applicant
Registration No. 32,933